# Lista de verificação de controles e conformidade

Para completar a lista de verificação de avaliação de controles, consulte as informações fornecidas no relatório de escopo, metas e avaliação de risco. Para mais detalhes sobre cada controle, incluindo o tipo e a finalidade, consulte o documento de categorias de controle.

Em seguida, selecione "sim" ou "não" para responder à pergunta: A Botium Toys tem esse controle atualmente em vigor?

**Lista de verificação de avaliação de controles**

|  |  |  |
| --- | --- | --- |
| **Sim** | **Não** | **Controle** |
|  |  | Menor Privilégio |
|  |  | Planos de recuperação de desastres |
|  |  | Políticas de senha |
|  |  | Separação de funções |
|  |  | Firewall |
|  |  | Intrusion detection system (IDS) |
|  |  | Backups |
|  |  | Antivirus software |
|  |  | Monitoramento manual, manutenção e intervenção para sistemas legados |
|  |  | Criptografia |
|  |  | Sistema de gerenciamento de senhas |
|  |  | Fechaduras (escritórios, vitrines, armazéns) |
|  |  | Closed-circuit television (CCTV) surveillance |
|  |  | Detecção/prevenção de incêndio (alarme de incêndio, sistema de sprinklers, etc.) |

Para completar a lista de verificação de conformidade, consulte as informações fornecidas no escopo, metas e relatório de avaliação de risco. Para mais detalhes sobre cada regulamentação de conformidade, revise os controles, estruturas e leitura de conformidade.

Em seguida, selecione "sim" ou "não" para responder à pergunta: A Botium Toys atualmente adere a esta melhor prática de conformidade?

**Compliance checklist**

Payment Card Industry Data Security Standard (PCI DSS)

|  |  |  |
| --- | --- | --- |
| **Sim** | **Não** | **Best practice** |
|  |  | Somente usuários autorizados têm acesso às informações do cartão de crédito dos clientes. |
|  |  | As informações do cartão de crédito são armazenadas, aceitas, processadas e transmitidas internamente, em um ambiente seguro. |
|  |  | Implemente procedimentos de criptografia de dados para proteger melhor os pontos de contato e os dados das transações de cartão de crédito. |
|  |  | Adote políticas seguras de gerenciamento de senhas. |

General Data Protection Regulation (GDPR)

|  |  |  |
| --- | --- | --- |
| **Sim** | **Não** | **Best practice** |
|  |  | Os dados dos clientes da U.E. são mantidos privados/seguros. |
|  |  | Existe um plano para notificar os clientes da UE dentro de 72 horas se seus dados forem comprometidos/houver uma violação. |
|  |  | Garantir que os dados sejam devidamente classificados e inventariados. |
|  |  | Aplique políticas, procedimentos e processos de privacidade para documentar e manter dados adequadamente. |

System and Organizations Controls (SOC type 1, SOC type 2)

|  |  |  |
| --- | --- | --- |
| **Sim** | **Não** | **Best practice** |
|  |  | Políticas de acesso do usuário são estabelecidas. |
|  |  | Dados sensíveis (PII/SPII) são confidenciais/privados. |
|  |  | A integridade dos dados garante que os dados sejam consistentes, completos, precisos e tenham sido validados. |
|  |  | Os dados estão disponíveis para indivíduos autorizados a acessá-los. |

Esta seção é opcional e pode ser usada para fornecer um resumo de recomendações ao gerente de TI sobre quais controles e/ou melhores práticas de conformidade a Botium Toys precisa implementar, com base no risco representado se não for implementada em tempo hábil.

Recomendações (opcional): Nesta seção, forneça recomendações, relacionadas a controles e/ou necessidades de conformidade, que seu gerente de TI poderia comunicar às partes interessadas para reduzir riscos aos ativos e melhorar a postura de segurança da Botium Toys.

Recomendações:

1. Implementação de Controles de Acesso: Adotar o princípio de "Menor Privilégio" e aplicar a separação de funções. Estes controles irão restringir o acesso a dados críticos somente aos funcionários autorizados.
2. Estabelecimento de Planos de Recuperação de Desastres e Backups: Implementar um plano de recuperação de desastres e procedimentos de backup regular para minimizar o tempo de inatividade e a perda de dados críticos em caso de eventos inesperados.
3. Sistemas de Detecção de Intrusões (IDS): Instalar um IDS para monitorar atividades suspeitas e detectar tentativas de invasão, aumentando a capacidade de resposta contra ameaças.
4. Reforço das Políticas de Senha e Gerenciamento de Senhas: Garantir que as políticas de senha atendam aos requisitos mínimos de complexidade e adotar um sistema de gerenciamento de senhas para reduzir a carga sobre o departamento de TI e melhorar a segurança.
5. Uso de Criptografia para Dados Sensíveis: Implementar a criptografia para proteger dados confidenciais, especialmente informações de cartões de crédito e dados pessoais de clientes, e aderir às normas do PCI DSS e GDPR para maior conformidade e segurança.